

Technická univerzita v Liberci
Hospodářská fakulta
katedra ekonomie

BAKALÁŘSKÁ PRÁCE

2007

Jan Šípek

Technická univerzita v Liberci
Hospodářská fakulta
katedra ekonomie

Studijní program: 6208 – Ekonomika a management
Studijní obor: Podniková ekonomika

Předpoklady rozvoje e-governmentu v ČR
a jeho dopad na podnikatelské prostředí

Progress of e-Government Implementation in the Czech Republic
and Its Impact on the Business Branch

JAN ŠÍPEK

Vedoucí práce: Ing. Aleš Kocourek, Ph.D.
katedra ekonomie
Konzultant: Ing. Filip Trešl
katedra ekonomie

Počet stran: 43
Počet příloh: 0

V Liberci dne 8. ledna 2007

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

V Liberci dne 8. ledna 2007

Jan Šípek

Poděkování

Děkuji Ing. Jaroslavu Kučerovi, informatikovi Krajského soudu v Ústí nad Labem pobočky Liberec, za konstruktivní rady, podnětné poznámky a ochotu podělit se o velmi cenné zkušenosti se zaváděním a používáním elektronických certifikátů.

Poděkování patří především mé manželce a dceři za velkou dávku pochopení a trpělivosti, kterou se mnou měly v době, kdy jsem čas, který patřil jim, věnoval této práci.

Resumé

Tato práce se zabývá otázkou rozvoje e-governmentu v České Republice a jeho dopadu na podnikatelskou sféru. Je patrné, že e-government doznal od svého počátku řady změn.

Pokouší se změny a pojem e-governmentu popsat a vysvětlit. Nastítnit současnou situaci a směry, kterými se ubírá (případně kam se možná bude ubírat do budoucna) a jimiž ovlivňuje podnikatelskou sféru.

Bakalářská práce poukazuje na průběh implementace a transformace vlády na „e-government“. Dále na současné legislativní normy a problematiku komunikace podniků s úřady. Část je věnována otázce bezpečnosti a důvěryhodnosti datových zpráv.

V souvislosti se čtyřletým výročím zavedení elektronického podpisu je možné považovat za přínos bakalářské práce především povědomost veřejnosti o obsahu a smyslu e-governmentu.

Bakalářská práce současně poukázala na aktuální problém teprve se rodící právní úpravy a nízkou nabídku služeb e-governmentu a tedy nízké využívání ze strany firem.

Summary

This work is about progress in e-government in the Czech Republic and its impacts on the business branch. It tries to describe and explain changes in e-government. The paper tries to show the present situation as well as the possible trends and directions of the future development and how e-government affects the business branch. It is evident e-government has gone through numerous changes from its beginning till now.

This Bachelor Work refers to implementation and transformation of government into e-government. It also refers to present legislative norms and problems in communication among firms and administrative departments. Part of this work has been devoted to electronic communication.

It also refers to present problems with insufficient legislative norms, low offer of services of e-government, and low usage by business branch.

In connection with the 4th anniversary of electronic signature it is possible to consider this work a basic source of information about e-government.

Klíčová slova

e-government

certifikační autorita

certifikát

elektronický podpis

elektronická podatelna

datová zpráva

Použité zkratky

EU..... Evropská unie

ICT Informační a komunikační technologie

ISVS.... Informační systém veřejné správy

MI..... Ministerstvo informatiky

SW..... software (programové vybavení)

ZoEP ... Zákon o elektronickém podpisu

Obsah

Úvod	12
1 Pojem „e-government“, přehled o současném stavu	13
2 Certifikační autority	19
2.1 Legislativní normy	19
2.2 Elektronický podpis	21
2.3 Certifikační autorita	22
3 Univerzální použitelnost, média	23
4 Bezpečnost dat	25
5 Dostupnost připojení k Internetu a náklady na výpočetní techniku ..	27
6 Počítačová gramotnost	30
7 Zefektivnění práce firem a jednotlivců	36
8 Příklady z praxe	38
8.1 Postup získání certifikátu u První certifikační autority	38
8.2 Elektronické tržiště pro informační a komunikační technologie do 2 milionů korun pro subjekty veřejné správy	39
Závěr	42
Použité zdroje	43
Elektronické zdroje:	43

Úvod

Cílem této práce je přinést přehled o rozvoji e-governmentu, jeho vzniku, cílech, principech, mechanismech a vývoji. Dále je cílem informovat čtenáře o legislativních normách, které tuto problematiku upravují, zejména problematiku certifikátů a elektronického podpisu a dále rovněž poukázat na důležitý aspekt bezpečnosti elektronické komunikace.

Po začlenění ČR do jednotného vnitřního trhu EU dochází k růstu tlaků konkurenčního prostředí na restrukturalizaci národní ekonomiky na úrovni makroekonomické i mikroekonomické. S tím vyvstává potřeba modernizace a zlepšení výkonu veřejné správy. Využívání informačních a komunikačních technologií (ICT) vede k růstu produktivity, zaměstnanosti, ke zlepšení kvality poskytovaných služeb a v neposlední řadě i k významným úsporám prostředků vynakládaných z veřejných rozpočtů.^[14]

Zajistit bezpečné, ekonomicky i geograficky dostupné moderní služby elektronických komunikací považuje vláda za základní předpoklad konkurenceschopnosti české ekonomiky. Bez toho nelze zajistit rovnocenné postavení české ekonomiky v rámci EU.

1 Pojem „e-government“, přehled o současném stavu

„e-Government představuje transformaci vnitřních a vnějších vztahů veřejné správy pomocí informačních a komunikačních technologií s cílem optimalizovat interní procesy. Jejím cílem je pak rychlejší, spolehlivější a levnější poskytování služeb veřejné správy nejširší veřejnosti a zajištění větší otevřenosti veřejné správy ve vztahu ke svým uživatelům.“¹

V roce 1999 byla schválena státní informační politika, která vymezuje poměrně široce a perspektivně oblast e-government služeb, tj. služeb státní a veřejné správy, poskytovaných prostřednictvím Informačního systému veřejné správy (ISVS) a ostatních komponent, o nichž se zmiňuje, resp. komponent, jejichž vybudování plánuje. Tento dokument stanovil celkem osm priorit, které pokrývaly následující tři oblasti:

- Informatizace veřejné správy.
- Informační gramotnost (vzdělávání).
- Elektronický obchod.

Realizace mnoha konkrétních úkolů, zejména z oblasti informatizace veřejné správy, byla bohužel ovlivněna nedostatkem finančních prostředků a rovněž obtížnou koordinací meziresortních aktivit.

Představy o budování „Státního informačního systému“ byly nahrazeny realističtější a modernější představou vzájemného propojení informačních systémů veřejné správy, které by poskytovaly širokou paletu služeb svým provozovatelům, celé veřejné správě a samozřejmě především veřejnosti. Tato představa byla následně podrobněji rozpracována v materiálu „Koncepce budování informačních

¹ Ministerstvo informatiky [online].[cit. 25. 8. 2006].

Dostupné z: <<http://www.micr.cz/egovernment/default.htm>>

systémů veřejné správy“ ještě z roku 1999 a vyústila ve vydání zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů.

Původní koncepce z roku 1999 byla zpracována ve dvou oblastech samostatně (formou dokumentů „Státní informační politika: cesta k informační společnosti“ dostupné z <http://www.esfcr.cz/clanek.php?lg=1&id=1277> a „Národní telekomunikační politika“ dostupné z <http://www.munet.cz/ismo/ntkp.htm>). Vláda se rozhodla respektovat úzkou provázanost a všeobecný trend spojení těchto dvou oblastí a vytvořit jeden společný strategický a koncepční dokument s názvem „Státní informační a komunikační politika – e-Česko 2006“ dostupné z <http://www.micr.cz/scripts/detail.php?id=275>.

K vypracování jednotné koncepce se vláda rozhodla před vstupem ČR do Evropské unie (EU). Jako členské země EU se České republiky týká evropský plán členských zemí „eEurope 2005: Informační společnost pro všechny“. Navrhovaná „Státní informační a komunikační politika“ se proto orientuje zejména na rozpracování záměrů a požadavků tohoto koncepčního dokumentu do národních podmínek tak, aby Česká republika dostala svým závazkům vůči EU a zároveň využila maximum možností, které skýtá potenciál ICT.

Vláda České republiky se ve svém programovém prohlášení z roku 2004 hlásí k cílům stanoveným v rámci tzv. lisabonského procesu.² K využití moderních ICT hodlá vláda ČR přistoupit jako k nástroji, pomocí něhož lze dosahovat růstu produktivity práce a celkové vzdělanosti, řešit celospolečenské problémy, jako je

² Na lisabonském summitu v březnu 2000 schválila Evropská rada strategický cíl přeměny Evropské unie do roku 2010 v nejkonkurenceschopnější a nejdynamičtější znalostní ekonomiku schopnou udržitelného růstu, s více a lepšími pracovními místy a s posílenou sociální soudržností. Podpora budování informační společnosti je přitom chápána jako jeden ze stěžejních kroků pro dosažení těchto cílů.

např. nezaměstnanost, začleňování znevýhodněných skupin občanů a nerovnoměrný rozvoj lidského potenciálu.

V této oblasti by se toho dalo mnoho vylepšit. Domnívám se, že pozornost současné i minulé vlády České republiky nebyla příliš soustředěna na tuto problematiku. Prakticky jediný větší projekt Internet do škol³ doprovázejí od počátku problémy, ať již ve výběru generálního dodavatele, tak v samotné realizaci projektu. Tento projekt má nepochybně velký význam, neboť se díky němu budou moci seznámit s počítači a Internetem i žáci dosud nevybavených škol. Česká republika bude v 1. pololetí roku 2009 předsedat Evropské unii. Dá se proto očekávat, že do té doby dojde k výraznému rozšíření nabídky služeb Portálu státní správy a k rychlejší modernizaci ICT ve státních institucích.

V roce 2000 byl přijat zákon o elektronickém podpisu,⁴ který vymezil právní rámec elektronické komunikace. Masivnějšímu rozšíření užívání elektronického podpisu stále brání řada překážek. Jde zejména o malou využitelnost e-podpisu ve veřejné správě (malý počet aplikací umožňujících transakční operace s veřejnou správou).

Změnu v tomto směru měl přinést „Portál veřejné správy“ spuštěný v roce 2003. Dá se říci, že nízká propagace tohoto portálu měla za následek počáteční nízké využívání ze strany firem a jednotlivců, neboť jednak nebyla k dispozici odpovídající nabídka služeb a také jediný elektronický podpis, který bylo možné získat od První certifikační autority za 700,- Kč, nebudil příliš zájem. Předpokládá se, že s větším rozšířením elektronického podpisu dojde i k většímu využívání Portálu veřejné správy. V současné době jsou na Portálu veřejné správy v aplikaci „Elektronická podání“ dostupné následující služby:

³ Jedná se o vybavení škol výpočetní technikou a připojením k Internetu.

⁴ Zákon o elektronickém podpisu č. 227//2000 Sb. ze dne 29. 6. 2000

a) Služby České správy sociálního zabezpečení

- Evidenční listy důchodového pojištění (pro období od 1.1.2004) - více informací na stránkách:
http://www.cssz.cz/tiskopisy/ELDP_2004/evidencni_listy_2004.asp
- Přihlášky/odhlášky (od 1.7.2005) - více informací na stránkách:
<http://www.cssz.cz/nemocenske/prihlasky/prihlasky.asp>
- Přehled o příjmech a výdajích OSVČ za rok 2005 (1. ledna 2006) - více informací na stránkách:
http://www.cssz.cz/osvc/prehled/prehled_osvc.asp

b) Služby Ministerstva informatiky ČR

- Roční výkaz o poštovních službách PS (MI)1-01 za rok 2005 - více informací na stránkách: <http://www.micr.cz/postovni/rvops.htm>

c) Služby Ministerstva financí - více informací o službách aplikace Elektronické podání pro daňovou správu na: <http://adis.mfcr.cz/adis/jepo/info/popis.htm>, v nabídce „EPO/Úvod/Vstupní informace“.

- Daň z přidané hodnoty
- Daň z příjmů fyzických osob
- Daň z příjmů právnických osob
- Příjmy ze závislé činnosti a funkčních požitků
- Daň silniční
- Daň z nemovitostí
- Oznámení podle §34 zákona č.337/1992 Sb.
- Hlášení platebního zprostředkovatele
- Obecné písemnosti určené pro finanční úřad

d) Služby Generálního ředitelství cel - celní správa - Intrastat. Více informací na stránkách: <http://www.cs.mfcr.cz>, odkaz Intrastat.

Pro veřejnou správu musí platit, že údaje, které jsou již jednou poskytnuty fyzickou nebo právnickou osobou orgánu veřejné správy, nemají být znovu zbytečně vyžadovány jiným úřadem. Tyto úřady si je v případě potřeby předají mezi sebou a teprve eventuální doplnění mohou požadovat po fyzických nebo právnických osobách a tato doplnění pak aktualizují v systému. Nesmí však docházet k bezdůvodnému opakování zapisování a ukládání těchto údajů.

To ovšem předpokládá, že orgány veřejné správy přistupují do centrálního systému, který má podobu např. základního registru obyvatel, základního registru ekonomických subjektů, základního registru územní identifikace nebo základního registru nemovitostí.

Dne 22. 11. 2006 vláda vzala na vědomí plán ministerstva financí, který počítá s tím, že přibližně od roku 2008 budou muset firmy přiznávat daň z přidané hodnoty přes internet, a odbourat tak posílání papírových formulářů. Povinná by byla elektronická přiznání pouze pro podniky s tržbami nad tři sta milionů korun ročně. Počítá se s tím, že podniky, kterých se tato povinnost bude týkat, již nyní využívají pro elektronické přiznání daně portál státní správy

Následující tabulka obsahuje fáze a úrovně transformace vlády na e-government, jak je nastínil Richard Heeks ve své knize *Implementing and Managing eGovernment*. **Chyba! Nenalezen zdroj odkazů.** Česká republika se nyní nachází na pomezí úrovně 1 a 2.

Tabulka č. 1.

– Stupně strategie řízení e-governmentu

	Stupeň 1	Stupeň 2	Stupeň 3	Stupeň 4
Název	Automatizace	Optimalizace	Re-engineering	Transformace
Změna	Změna technologie z manuální na IT prostřednictvím automatizace	Změna aplikací uspořádáním datových struktur a pracovních procesů	Změna organizace pomocí překonstruování datových struktur a pracovních procesů	Změna organizace pomocí kompletní transformace datových struktur a pracovních procesů
Organizační zaměření	Operační/úřednická úroveň	Taktická úroveň managementu	Strategická úroveň managementu	Klienti (a/nebo "konkurenti")
Typický manažerský problém	Zprovoznit e-government a udržet jej v chodu	Kontrola nákladů a pracovníků systémů e-governmentu	Koordinovat systém e-governmentu napříč celou organizací	Uzpůsobit e-government tak, aby splňoval požadavky klientů
Pohled na informace	Malý průzkum informací	Manažerský nástroj	Organizační prostředek	Strategický/konkurenční prostředek
Dlouhodobé cíle	Efektivita: děláni stejných věcí stejnou cestou, ale rychleji nebo levněji	Vzrůstající efektivita: děláni stejných věcí lepším způsobem	Radikální efektivita: děláni stejných věcí radikálně rozdílným způsobem	Transformace: děláni nových věcí

Zdroj: Richard Heeks - Implementing and Managing eGovernment

2 Certifikační autority

2.1 Legislativní normy

Pro úspěšnou komunikaci se státní správou je zapotřebí vlastnit certifikát vydaný akreditovanou certifikační firmou, který pak lze použít k elektronickému podpisu datové zprávy. Tuto problematiku legislativně upravuje:

- **Zákon o elektronickém podpisu č. 227//2000 Sb.** ze dne 29. 6. 2000. Upravuje používání elektronického podpisu a poskytování souvisejících služeb, kontrolu povinností stanovených tímto zákonem a nastiňuje základní podmínky udělení statutu akreditovaný poskytovatel certifikačních služeb. Definuje rozdíl mezi certifikátem obecným a kvalifikovaným^[5]
- **Nařízení vlády č. 304/2001 Sb.** ze dne 25. 7. 2001. Doplnuje Zákon o elektronickém podpisu (ZoEP), zejména v oblasti činnosti elektronických podatelů v rámci orgánů veřejné moci tak, aby bylo zajištěno přijímání podání v elektronické podobě při využití kvalifikovaných certifikátů dle výše uvedeného zákona.^[4]
- **Vyhláška Úřadu pro ochranu osobních údajů č. 366/2001 Sb.** ze dne 3. 10. 2001. Upřesňuje podmínky § 6 ZoEP specifikující povinnosti poskytovatele certifikačních služeb vydávajícího kvalifikované certifikáty a § 17 ZoEP, který definuje prostředky pro vytváření a ověřování zaručených elektronických podpisů.^[6]
- **Zákon č. 226/2002** ze dne 9. 5. 2002 Mění § 11 ZoEP upravujícího podmínky používání elektronického podpisu a certifikátů v oblasti orgánů veřejné moci.^[7]
- **Zákon č. 517/2002** ze dne 14. 11. 2002. Upravuje ZoEP na základě provedení některých opatření v soustavě ústředních orgánů státní

správy, nahrazení slova „Úřad pro ochranu osobních údajů“ a „Úřad“ slovem „Ministerstvo informatiky“.^[8]

- **Zákon č. 440/2004** ze dne 24. 6. 2004. Upravuje ZoEP specifikující podmínky poskytování zaručeného elektronického podpisu, elektronických značek a kvalifikovaných systémových certifikátů^[9]
- **Nařízení vlády** ze dne 25. 8. 2004. Stanovuje povinností orgánů veřejné moci zřídit e-podatelný (nebo v případě malého objemu elektronické komunikace zajistit příjem a odesílání zpráv prostřednictvím e-podatelný jiného řadu), vybavit příslušné zaměstnance zaručenými elektronickými podpisy a zajistit odpovídajícím způsobem ochranu zpracovávaných informací. Nařízení vlády nabylo účinnosti k 1. lednu 2005.

Uvedené legislativní normy upravují tuto problematiku poměrně zešíroka a velmi obecně. V praxi se ukázalo, že je potřeba k těmto normám vydat prováděcí předpisy a metodické pokyny. Řada organizací měla a stále má problémy s tím, jak vlastně má fungovat elektronická podatelna, jakým způsobem mají reagovat na elektronická podání, jakým způsobem mají s elektronickým podáním nakládat – ať již se jedná o předání odpovědným pracovníkům, zálohování zpráv, archivaci apod.

Například ministerstvo spravedlnosti teprve v roce 2006 zřídilo resortní skupinu, která má za cíl vytvořit směrnici k provozu elektronických podatelen. Dalším cílem této skupiny je vybrat aplikaci, která by v maximální míře zjednodušila provoz elektronické podatelny, a doporučit ji složkám resortu k zakoupení. Toto řešení však má být pouze dočasné, neboť se plánuje implementovat v roce 2007 aplikaci centrální elektronické podatelny. Tím by měly zmizet problémy spojené s různým programovým vybavením na jednotlivých složkách resortu a mělo by být dosaženo jednotného způsobu vyřizování elektronických podání..

2.2 Elektronický podpis

„Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě.

Zaručeným elektronickým podpisem se rozumí elektronický podpis, který splňuje následující požadavky:

- 1) je jednoznačně spojen s podepisující osobou,
- 2) umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- 3) byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- 4) je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat.“⁵

Elektronický podpis je tedy takovým ekvivalentem pečeti. Příjemce tak může poznat, zda došlo k porušení pečeti a pozměnění zprávy, a zda tedy může, nebo nemůže zprávě důvěřovat. Tento princip je hojně používán v elektronickém styku s bankovními institucemi, které elektronické certifikáty využívají již delší dobu.

Stát pro potřeby elektronické komunikace uznává zaručený elektronický podpis založený na kvalifikovaném certifikátu. To znamená, že je možné ověřit, že datovou zprávu podepsala osoba uvedená na tomto kvalifikovaném certifikátu a že lze říci, zda zpráva nebyla mezi dobou podpisu a přijetím na elektronické podatelně změněna.

⁵ Zákon o elektronickém podpisu č. 227/2000 Sb. ISSN 1211-1244

2.3 Certifikační autorita

K používání elektronického podpisu je nutný kvalifikovaný certifikát vydaný akreditovanou certifikační autoritou. Certifikační autorita je fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci. Kvalifikovaný poskytovatel certifikačních služeb je poskytovatel, kterému byla udělena akreditace podle zákona o elektronickém podpisu.

V České republice existují v současné době tři akreditované certifikační společnosti, jsou to:

- První certifikační autorita, a.s. – od 18. 3. 2002
 - o Certifikát je nabízen za 632,- Kč bez DPH a má platnost 1 rok
- eIdentity a. s. – od roku 2004
 - o Certifikát je nabízen za 590,- Kč bez DPH a má platnost 1 rok
- Česká pošta, s.p. PostSignum QCA – od 3. 8. 2005
 - o Certifikát je nabízen za 160,- Kč bez DPH a má platnost 1 rok

Všechny tyto společnosti nabízejí kvalifikované certifikáty ve smyslu zákona o elektronickém podpisu, a tyto certifikáty jsou tedy uznávány portálem státní správy a všemi státními institucemi, které mají zřízenou elektronickou podatelnu. Pro firmy a jednotlivce se liší v podstatě pouze cenou, dostupností výdejních míst a samotným procesem vydání elektronického certifikátu. ^{[10][11][12]}

Působí zde ještě další certifikační autority, ale ty zatím nemají akreditaci podle zákona o elektronickém podpisu, a jimi vydané certifikáty tedy nemohou být použity pro komunikaci s úřady ve smyslu tohoto zákona.

3 Univerzální použitelnost, média

Nové technologie umožňují vytvářet moderní a efektivní veřejnou správu, která nabízí nové nebo vylepšené služby. Služby veřejné správy musí být pro uživatele jednoduché a musí být všem dostupné.

Aby bylo možné využívat služby e-governmentu v masovém měřítku, je nutné, aby tyto služby byly co nejvíce univerzální. To znamená, aby byly sjednoceny standardy používaných médií, včetně datových formátů. V současné době existuje velké množství médií a datových formátů a není technicky a finančně možné, aby každý úřad byl vybaven pro přijetí každého z nich. Současná legislativa tuto problematiku upravuje dosti volně, záleží víceméně na konkrétních institucích státní správy, jaký k tomuto problému přijmou vnitřní prováděcí předpis nebo směrnici. Portál veřejné správy upravuje tuto problematiku ve svém provozním řádu v kapitole 4.1 Formát a přenos podání^[16]

Jako nejvhodnější se jeví použití elektronických formulářů poskytovaných samotnými institucemi státní správy prostřednictvím webových aplikací. Ne všechny informace je ale možné poskytnout prostřednictvím těchto formulářů. Např. v případě doložení písemností při založení společnosti je potřeba tyto zaslat elektronickou formou. Tato služba však zatím není prostřednictvím portálu státní správy možná, ale v případě budoucího zavedení by mohla narážet právě na problém nejasné úpravy akceptovaných datových zpráv. Vláda České republiky by tedy neměla tuto problematiku podceňovat a měla by jí věnovat patřičnou pozornost.

Samotné určení, jaké formáty datových zpráv a jaká datová média instituce akceptuje, je ponecháno na vlastníkově dané služby. Státní správa je v naprosté většině vybavena počítači typu PC IBM a programovým vybavením firmy Microsoft, a ve většině případů tedy nemá problémy s přijetím nejběžnějších formátů

datových zpráv a datových médií. Každá organizační složka si sama určuje vnitřní směrnici, jaké zprávy akceptuje. Např. Krajský soud v Ústí nad Labem na svých internetových stránkách sděluje:

„Datové zprávy jsou přijímány ve formátech: xls, doc, rtf, txt, pdf, 602, wpd, jpg, gif (bez vnitřních programových kódů - maker). Elektronicky podepsaná podání se přijímají ve formátu *.msg. Komprimované soubory lze posílat ve formátech: zip, rar, arj. Z důvodu bezpečnosti počítačové sítě neakceptujeme přípony: exe, pif, com, vb?, bat, lnk, scr, whs, cmd. Ostatní soubory lze na elektronickou adresu soudu zaslat s rizikem, že mohou být vráceny, neboť soud nemá programové prostředky na jejich otevření. Datové zprávy jsou přijímány na disketách, CD, DVD nebo USB Flash disku (tzv. palec).“⁶

⁶ Informační server českého soudnictví - Krajský soud v Ústí nad Labem – [online].[cit. 8. 12. 2006]. Dostupné z: <<http://portal.justice.cz/soud/soud.aspx?j=32&o=22&k=370&d=31374>>

4 Bezpečnost dat

Výměna informací v elektronické podobě je trendem dnešní doby. Prudký rozmach informačních a komunikačních systémů, který zasahuje do všech oblastí lidské činnosti, a jejich široká dostupnost zvyšují riziko napadení těchto systémů, a to ať záměrně, náhodně, nebo v důsledku chyby, případně neznalosti.^[1]

Ne každá informace je však určená pro každého. Pokud se jedná o elektronické transakce ve sféře státní správy, financí, zdravotnictví, obchodu, dopravy a služeb apod., je nutné, aby byly stejně důvěryhodné jako klasické procedury prováděné na základě osobního styku používajícího postupy ověřování totožnosti, vlastnoruční podpisy a archivaci dokumentů.

Aby bylo dosaženo předchozích podmínek, je nutné, aby bezpečnostní cíle plnily následující body:

- **důvěrnost informací** Systém musí zajistit, že neautorizované subjekty nezískají přístup k důvěrným informacím.
- **integrita** Systém musí zabezpečit informace proti neautorizované modifikaci.
- **neodmítnutelnost odpovědnosti** Systém musí zajistit schopnost přesvědčit třetí nezávislou stranu o přímé odpovědnosti subjektu za odeslání, případně přijetí zprávy.

Ochrana datového přenosu, tj. trasy mezi místem odeslání a přijetí, je velice náročná a většinou nemožná. Prakticky nelze zajistit, aby po celé délce linky nedošlo k odposlechu předávané informace. Zde se nabízí možnost logické ochrany dat, neboli šifrování. Znamená to zašifrovat data na straně odesílatele, odeslat je a dešifrovat na straně příjemce. Tak je zaručeno, že v případě neautorizovaného přístupu ke zprávě, nemá tato osoba možnost přečíst posílaná data.

To je samozřejmě zajištěno pouze za předpokladu, že odesílatel zprávu zašifruje a že nedojde ke zneužití použitého šifrovacího klíče. Zde přichází na řadu nutnost zabezpečení podnikových sítí a samotných pracovních stanic proti neoprávněnému vniknutí cizí osoby.

V případě uložení klasických papírových dokumentů, kdy jsou tyto uloženy v nejlepším případě v uzamčeném a střeženém archivu, je pro případného útočníka složité se k těmto dokumentům dostat. V případě uložení elektronických dokumentů útočník nemusí fyzicky pro tyto dokumenty dojít. Avšak současné možnosti ochrany datových úložišť jsou již natolik pokročilé a účinné, že prakticky znemožňují neoprávněnou manipulaci s elektronickými údaji.

Nejvíce se používá HW zabezpečení sítí pomocí konfigurovatelných síťových prvků jako jsou switche a firewally (např. produkty firem 3com, Cisco). SW zabezpečení je zastoupeno vestavěnými bezpečnostními mechanismy operačních systémů (integrovaný firewall systému MS Windows od firmy Microsoft), případně SW produktů třetích firem jako jsou firewally a antivirové programy (např. produkty firem Symantec, Kerio Technologies, Grisoft apod.)

5 Dostupnost připojení k Internetu a náklady na výpočetní techniku

Využívání služeb e-governmentu je podmíněno vlastnictvím ICT a přístupem k Internetu. Současná nabídka výpočetní techniky a připojení k internetu je velice široká, a není tedy problém, aby si z ní každý vybral to, co mu nejlépe vyhovuje. Ačkoli cena výpočetní techniky rok od roku klesá, je stále ještě pro mnohé příliš vysoká, a brání tak samotnému pořízení ICT.

Cena osobního počítače s odpovídajícím programovým vybavením se pohybuje okolo 14 000,- bez DPH. Přitom v roce 2001 byla cena přibližně 25 000,- Kč bez DPH.⁷ Zde je vidět příznivý trend v poklesu cen výpočetní techniky.

Nejinak je tomu i s nabídkou připojení k internetu. Ta je také velice široká a zahrnuje možnost připojení pomocí pevné telefonní linky, mobilního telefonu, bezdrátové technologie, satelitní technologie, pevným připojením nebo připojením pomocí elektrické rozvodné sítě. Ne všechny technologie jsou však dostupné na celém území ČR. V současné době se jako nejjednodušší jeví připojení pomocí běžné telefonní linky, neboť tu využívá naprostá většina firem i domácností.

Pro srovnání je uveden přehled nabídek několika poskytovatelů (jedná se o připojení technologií ADSL rychlostí 512 kbp/s, což je pro komunikaci se státní správou více než dostačující):

⁷ Při stanovení přibližné ceny jsem vycházel z ceníků prodejců výpočetní techniky (OZO, s. r. o., LSC s. r. o., LOSAN s. r. o., 100Mega Liberec spol. s r. o.) platných v roce 2001 a v listopadu 2006.

Společnost	Cena připojení (bez DPH)	Zdroj
Skynet, a.s.	379,-	http://www.skynet.cz/
GTS Novera, a.s.	395,-	http://www.gtsnovera.cz/
TISCALI Telekomunikace Česká republika s.r.o.	395,-	http://www.tiscali.cz/home/
Telefónica O2 Czech Republic, a.s.	399,-	http://www.cz.o2.com/fixed/cz/firmy/index.html
Czech Online, a.s.	1 190,-	http://firmy.volny.cz/products/
Radiokomunikace, a.s.	1 890 až 2 490,- ⁸	http://www.radiokomunikace.cz/cs/firmy.ep/

Zdroj: [vlastní]

Tato nabídka je dostupná z webových stránek zmíněných společností a údaje jsou z 9. 12. 2006. Jedná se o měsíční paušál za připojení. K ceně je nutné připočítat ještě paušál za pevnou telefonní linku společnosti Telefónica, který činí 339,- Kč bez DPH. Celkem tedy vyjde nejlevnější připojení k internetu technologií ADSL na 718 Kč bez DPH měsíčně. V roce 2003, kdy bylo poprvé možné objednat trvalé připojení k internetu, byla nabídka velice omezená. Toto připojení bylo možné objednat pouze v Praze, Brně a Ostravě. Nejnižší cena, za jakou bylo ADSL nabízeno, byla 1 237,- Kč bez DPH u nejnižší rychlosti a 11 349,- Kč bez DPH u nejvyšší rychlosti.⁹

Náklady firmy na ICT pro komunikaci se státní správou se tedy pohybují přibližně ve výši 14 000 Kč bez DPH za pořízení počítače s odpovídajícím

⁸ Cena závisí na tom, zda firma má nebo nemá pevnou telefonní linku a na smluveném měsíčním hovorném.

⁹ Živě.cz – ADSL: Jak, u koho a za kolik – [online].[cit. 7. 3. 2003]. Dostupné z: <http://www.zive.cz/h/Uzivatel/Ar.asp?ARI=109671&CAI=>>

programovým vybavením, 700 Kč bez DPH za měsíční paušál připojení k internetu pomocí technologie ADSL a 460 Kč bez DPH za kvalifikovaný certifikát vydaný akreditovanou certifikační autoritou.¹⁰

¹⁰ Při stanovení přibližné ceny jsem vycházel z ceníků prodejců výpočetní techniky (OZO, s.r.o, LSC s. r. o., LOSAN s. r. o., 100Mega Liberec spol. s r. o.) platných k listopadu 2006.

6 Počítačová gramotnost

Jedním ze stěžejních faktorů udržení a rozvoje národního hospodářství je informační vzdělanost. Podle výzkumů a studií mnoha evropských zemí a mezinárodních organizací¹¹ se ukazuje, že rozvoj evropské ekonomiky závisí na přechodu od ekonomiky orientované na výrobu k ekonomice založené na efektivním využívání a předávání znalostí a informací.

Mezi hlavní bariéry využívání počítače a internetu patří zejména nedostatečná představa o jejich možnostech a také strach z počátečních kroků. Dalším problémem je nízká dostupnost ICT produktů a služeb, daná jejich relativně vysokou cenou vzhledem ke kupní síle. Vláda České republiky považuje rozvoj počítačové gramotnosti za klíčový pro rozvoj celé ekonomiky a společnosti vůbec.

Ministerstvo informatiky proto zadalo agentuře STEM/MARK výzkum počítačové gramotnosti. Cílem výzkumu bylo rozdělit populaci ČR z hlediska využívání, gramotnosti a plánovaného využívání ICT. Dále otestovat počítačové dovednosti a schopnosti, získat zpětnou vazbu na realizované kroky koncepce informační politiky, odkrýt bariéry bránící širšímu využití ICT v komunikaci s úřady a veřejnou správou a definovat „informační/počítačovou gramotnost“ pro možnou kvantifikaci s možností sledování změn v čase. Výsledky byly prezentovány dne 25. 8. 2005. Výzkum byl proveden na vzorku 16 000 respondentů ve věku mezi 18 a 60 lety.

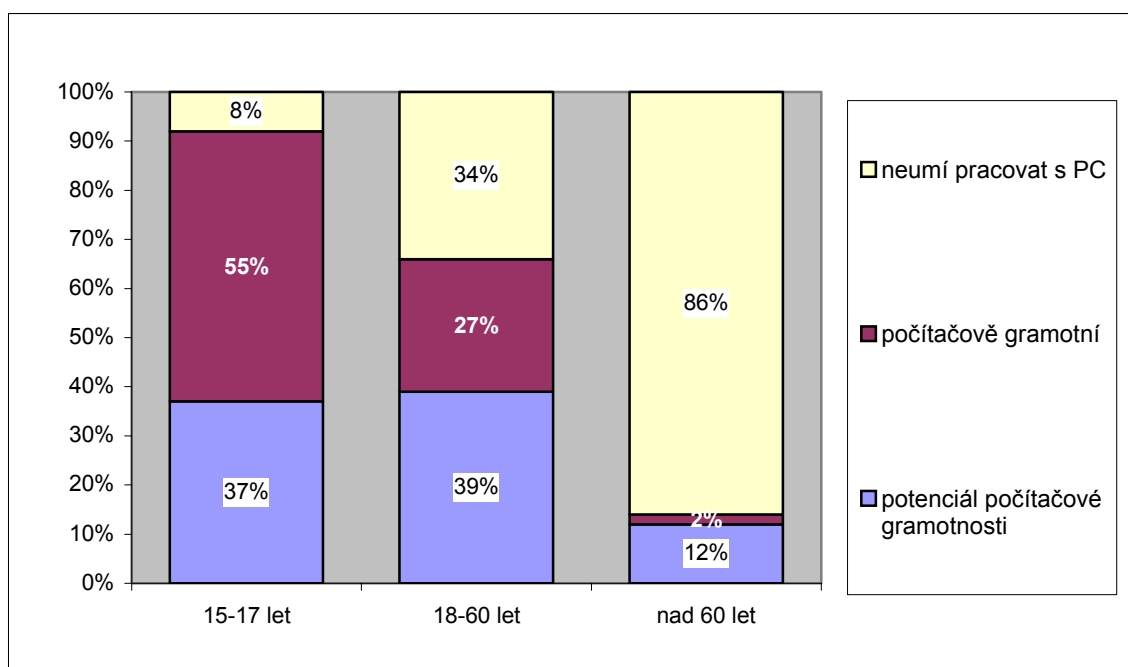
¹¹ Např. - Rozhodnutí č. 2318/2003/ES Evropského parlamentu a rady ze dne 5. prosince 2003; The Work Foundation – Defining the knowledge economy; OECD – Strategic Investment Promotion – Successful Practice in Building Competitive Strategies

Realizátoři průzkumu (agentura STEM/MARK) rozlišují mezi informační a počítačovou gramotností:

- Informační gramotnost je schopnost rozeznat, kdy potřebuji informace, umět je vyhledat, vyhodnotit a efektivně využít.
- Počítačová gramotnost je schopnost pracovat s ICT, schopnost používat internet ke komunikaci, k vyhledávání a zpracování informací. Dále schopnost efektivního využití služeb a možností, které ICT nabízí.

Podrobný průzkum využívání služeb e-governmentu zatím nebyl proveden, ale následující grafy dávají alespoň částečnou představu o tom, zda existuje potenciál využití těchto služeb.

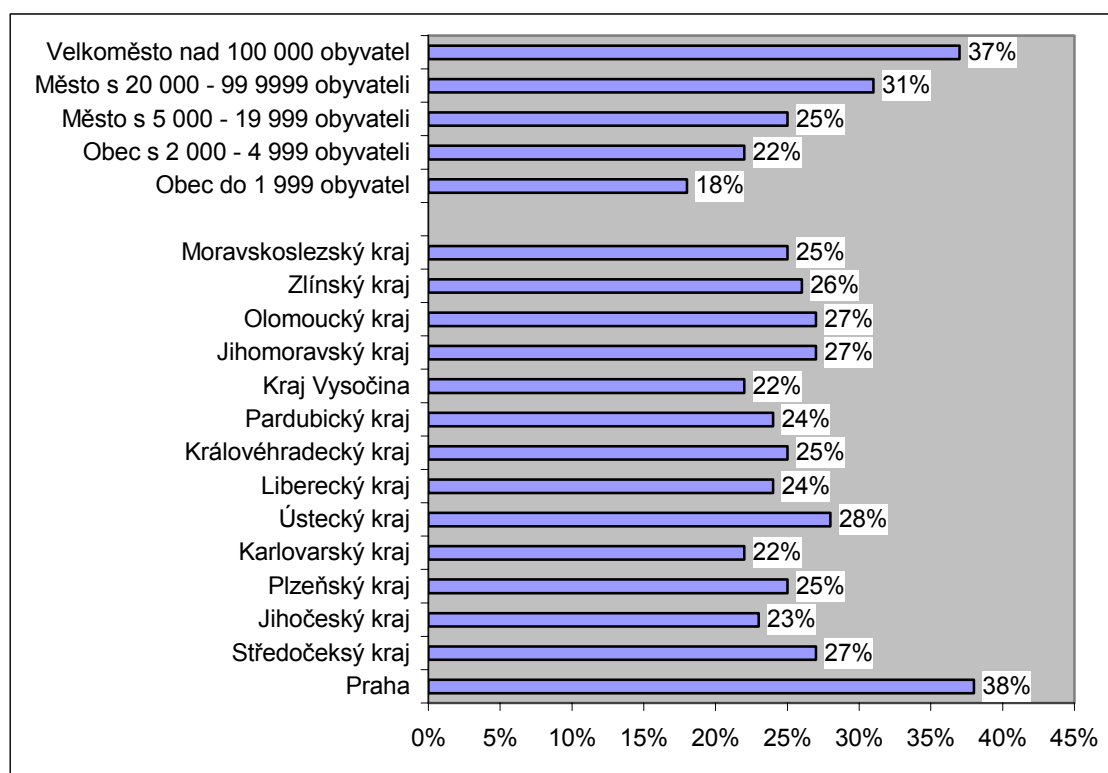
Graf č. 1. - Potenciál počítačové gramotnosti v ČR



Zdroj: STEM/MARK, Výzkum informační gramotnosti: 08/2005

Z tohoto grafu je nejdůležitější skupina 18-60 let, kde je 27 % dotázaných počítačově gramotných. Celá třetina však neumí s PC pracovat. 39 % dotázaných vykazuje potenciál počítačové gramotnosti, což znamená, že tyto osoby využívají počítač, avšak ne na úrovni alespoň minimální počítačové gramotnosti. Do budoucna je ale možnost, že tato skupina své znalosti rozšíří.

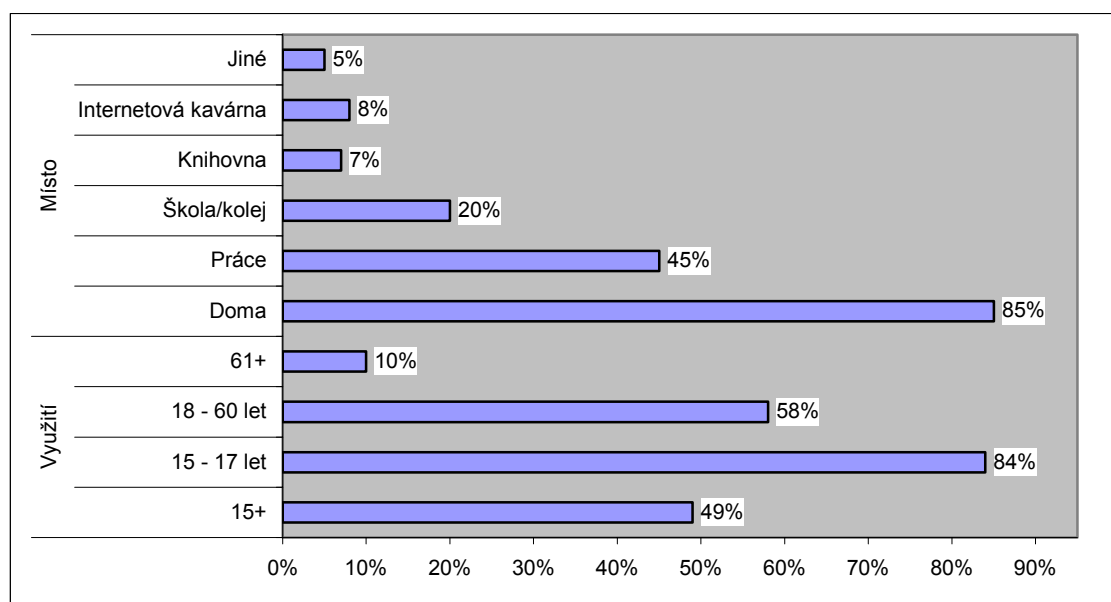
Graf č. 2. - Počítačová gramotnost podle regionů



Zdroj: STEM/MARK, Výzkum informační gramotnosti: 08/2005

Z Grafu 2 vyplývá, že počítačová gramotnost je doménou větších měst. Průměr 27 % dosahují pouze města s více než 20 000 obyvateli a pouze 4 kraje ze 14.

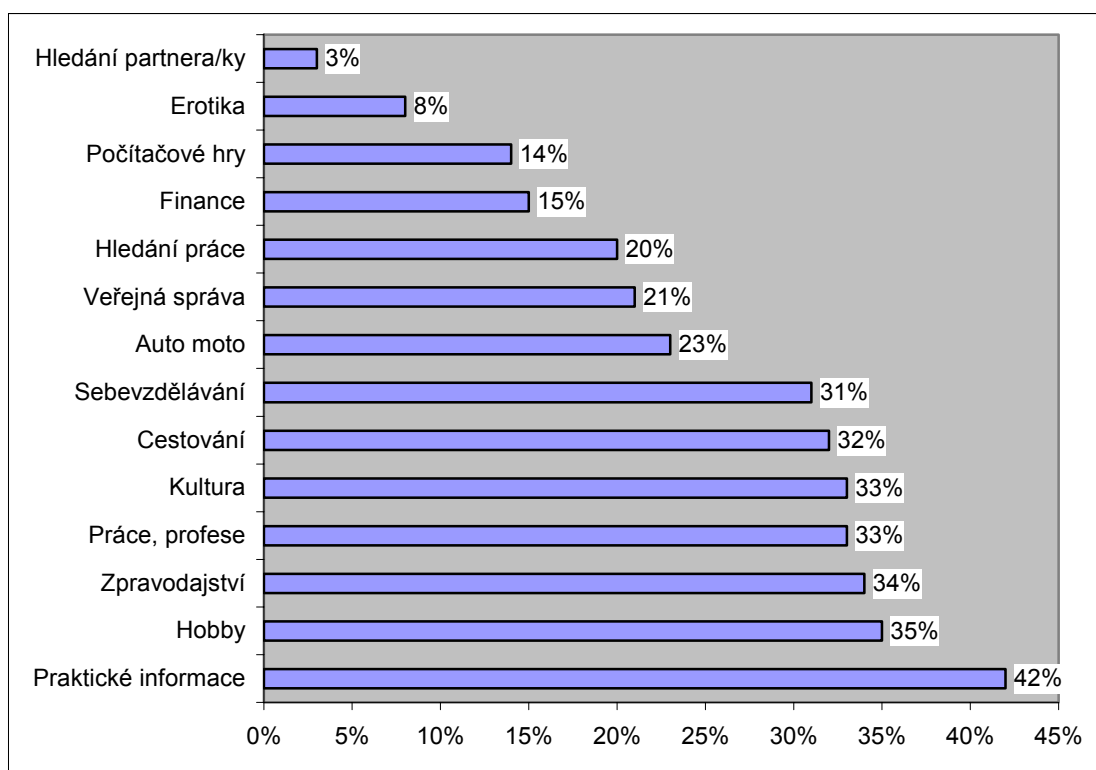
Graf č. 3. Využití stolního počítače



Zdroj: STEM/MARK, Výzkum informační gramotnosti: 08/2005

Počítač používá 58 % dotázaných ve věku 18 – 60 let, z nich téměř polovina (45 %) ho používá k práci. Podle průzkumu Use of the Internet among individuals and enterprises statistického úřadu Evropské komise Eurostat provedeného v roce 2005 použilo v České republice 33 % zaměstnaných osob Internet alespoň jednou týdně. Přičemž průměr Evropské unie je 55 %. Česká republika tedy poměrně zaostává za evropským průměrem. Například ve Velké Británii je to 64 % zaměstnaných osob a v Nizozemsku dokonce 85 %. Podle stejného průzkumu má v České republice 92 % společností připojení k Internetu, z toho 52 % společností využívá širokopásmové připojení (průměr EU je přitom 63 %). 92 % českých společností tedy má k dispozici počítač, avšak podle průzkumu agentury STEM/MARK využívá počítač pro práci pouze 45 % osob ve věku 18 – 60 let.

Graf č. 4. Využití Internetu v dotázané skupině



Zdroj: STEM/MARK, Výzkum informační gramotnosti: 05/2005

Graf 4 ukazuje, že pouze 21 % dotázaných využívá internet pro komunikaci s veřejnou správou. To je poměrně nízké procento s ohledem na předchozí graf, který dával středně vysoké využívání ICT k práci (45 %).

Vláda ČR považuje rozvoj informační gramotnosti za klíčový pro řešení současných problémů v ekonomické i sociální oblasti. Informační gramotnost bude čím dál významnější součástí celkové vzdělanosti a bude stále více rozhodovat o kvalitě života i možnostech uplatnění. Absence či nedostatek informační gramotnosti vytváří silný handicap, který může vést k rozdělení obyvatelstva. Jde o nebezpečí tzv. "digital divide". Je tedy naprosto nezbytné proti tomuto nebezpečí bojovat formou odstraňování překážek a podporou možností celoživotního vzdělávání.

7 Zefektivnění práce firem a jednotlivců

e-Government obecně přináší zefektivnění práce zejména díky časové úspoře pro podnikatele, který nemusí trávit dlouhé hodiny vyřizováním věcí na úřadech a může vše provést ze své firmy pomocí počítače. Také zefektivňuje práci státních institucí, neboť zaváděním elektronických rejstříků a databází usnadňuje vyhledávání a předávání informací v nich obsažených mezi jednotlivými orgány veřejné správy. Nepřímo ovlivňuje zvyšování produktivity práce prostřednictvím tlaku na zavádění moderních ICT do podniků.

Vláda ČR si uvědomuje nutnost udržení konkurenceschopnosti mezi zeměmi EU a zprostředkovává prostřednictvím internetových stránek Portálu veřejné správy důležité informace, které jinak podnikatel musí získat studiem dostupné literatury, jedná se např. o informace týkající se založení nebo zrušení společnosti, informace o veřejných zakázkách, informace o daňovém systému, informace týkající se pracovněprávních vztahů apod.

V ČR je však nabídka služeb e-governmentu zatím nízká, je to dáno tím, že e-government v ČR prošel teprve krátkým vývojem a má před sebou dlouhou cestu, než bude legislativní i obsahová stránka na úrovni srovnatelné s ekonomicky vyspělejšími zeměmi, které již na transformaci „papírové vlády“ na e-government pracují řadu let. Ve Velké Británii již v roce 1990 vytvořili Central IT Unit (Centrální IT útvar). Ten převzal část činností od Central Computer and Telecommunications Agency (Centrální počítačová a telekomunikační agentura), která tak získala větší poradenskou a implementační roli, do té doby příliš slabou na udržení pozice nezávislé jednotky. V současné době nabízí vládní portál Velké Británie více než 100 služeb s přibližně 8 miliony aktivních přihlášení. Zatímco v České republice se

od zahájení provozu do 31. 7. 2006 přihlásilo ke službám Portálu veřejné správy 50 000 uživatelů.¹²

¹² Údaje o uživatelích Portálu veřejné správy převzaty z případové studie „Elektronická podání na Portálu veřejné správy využívá už 50 000 uživatelů“. Dostupné z http://www.microsoft.com/cze/casestudies/micr_50000.msp

8 Příklady z praxe

8.1 Postup získání certifikátu u První certifikační autority.

1. Prvním krokem je instalace kořenového certifikátu certifikační autority do počítače, který bude používán pro elektronickou komunikaci.
2. Následuje vytvoření žádosti o vydání certifikátu. To se provádí pomocí formuláře na stránkách:
http://www.ica.cz/home_cs/?acc=zadost_kvalifikovany_certifikat
3. Po vyplnění požadovaných údajů dojde k vytvoření žádosti, kterou je nutné uložit na datové médium a doručit na kontaktní místo. V Liberci má První certifikační autorita umístěna pracoviště na pobočkách Československé obchodní banky, a.s. na tř. 1. Máje 18 a ve Frýdlantské ulici, č. p. 15 a dále na Obchodním místě RM-SYSTÉMU ve Voroněžské ulici, č. p. 144.
4. Na kontaktním místě je ověřena totožnost žadatele o certifikát, a pokud je žádost dodaná na datovém médiu a ověření totožnosti v pořádku, pracovník kontaktního místa provede vytvoření certifikátu. Celá operace trvá jen několik minut.
5. Vydaný certifikát je nutné zavést zpět do počítače, na kterém byla žádost vygenerována. Po tomto kroku je možné začít certifikát používat k elektronickému podpisu.

Doporučuje se provést zálohu soukromého klíče, který pak může být použit pro reinstalaci certifikátu v případě poškození počítače, na kterém byl původně nainstalován.

8.2 Elektronické tržiště pro informační a komunikační technologie do 2 milionů korun pro subjekty veřejné správy

Na základě usnesení vlády České republiky č. 683 ze dne 26. června 2002, o opatřeních ke koordinovanému vynakládání finančních prostředků na informační a komunikační technologie, zajišťuje Ministerstvo informatiky ČR provoz elektronických tržišť pro státní správu. Licenci MI k provozování e-tržiště mají tito tři provozovatelé:

B2B Centrum, a.s. - <https://gem.b2bcentrum.cz/softrade/>

CenTrade, a.s. - <http://www.centrade.cz/>

ECONOMY.CZ s.r.o. - <http://www.allytrade.cz/GeMDefault.asp>

Dnem 1. ledna 2007 došlo ke zrušení společnosti CenTrade, a.s., IČ: 26513731, se sídlem Praha 3, Olšanská 55/5, PSČ 130 00 (dále jen „CenTrade“). Společnost CenTrade, která byla součástí skupiny Telefónica O2, je v současné době v likvidaci.

Spolu s ukončením podnikatelských aktivit společnosti CenTrade dojde také k uzavření elektronického tržiště CenTrade. Na základě Smlouvy o poskytování služeb Elektronického tržiště CenTrade (dále jen „Smlouva“) bude v souladu s příslušnými ustanoveními Smlouvy přistupováno v průběhu března 2007 k výpovědi této Smlouvy. Výpovědní lhůta počne běžet prvním dnem kalendářního měsíce následujícího po doručení výpovědi a činí tři měsíce.¹³

¹³ Internetové stránky elektronického tržiště CenTrade – [online].[cit. 2. 3. 2007]. Dostupné z: <<http://www.centrade.cz/>>

E-tržiště B2B Centrum, a.s.

Provozovatel tohoto tržiště získal jako první licenci k provozování a spustil tržiště dne 1. 9. 2002. Statistika tržiště ze dne 8. 12. 2006 udává, že tržiště využívá 1 167 odběratelů (tedy institucí státní správy) a 3 535 dodavatelů. Uzavřených obchodů na tomto tržišti je 27 804.

Odběratel

Odběratelem na e-tržišti státní správy je státní instituce. Ta se zaregistruje jako odběratel a po přidělení uživatelského jména a hesla může začít nakupovat ICT prostřednictvím tržiště. Nákup probíhá prostřednictvím výběrového řízení, kdy odběratel zadá podmínky obchodu jako je požadovaná dodací lhůta, platnost nabídky, splatnost, zda požaduje dovoz zboží na místo doručení atd. Poté vyplní termín podání nabídek a termín plánovaného vyhodnocení. Následuje zadání požadovaného zboží, které je možné vybrat z nabízeného katalogu nebo zapsat ručně.

Zbývá už jen vybrat jednoho či více dodavatelů, kterým bude zaslána poptávka a čekat na zaslání nabídky. Po obdržení nabídky zbývá pouze vybrat vítěze výběrového řízení podle zadaných kritérií, jako je nejnižší cena za položku, za nabídku celkem, cena za dopravu atd. Vítězná firma je informována e-mailem o tom, že vyhrála výběrové řízení a další komunikace mezi státní institucí a touto firmou již probíhá klasickým způsobem (ať již telefonicky nebo e-mailem).

Dodavatel

Dodavatelem je zde firma prodávající ICT, která po registraci a sepsání zprostředkovatelské smlouvy s provozovatelem e-tržiště může nabízet své zboží. Z pohledu dodavatele probíhá operace na e-tržišti následovně:

- nejprve obdrží od odběratele poptávku, na kterou může nebo nemusí reagovat (např. nevede požadované zboží, nestihne včas reagovat v požadované lhůtě atd.),
- pokud se rozhodne reagovat, vyplní k poptávanému zboží svou cenu a odešle nabídku zpět odběrateli,
- po vyhodnocení výběrového řízení odběratelem je dodavatel informován o tom, zda řízení vyhrál či nikoli,
- pokud je dodavatel vítězem tohoto výběrového řízení, potvrdí odběrateli telefonicky nebo e-mailem termín dodání objednaného zboží, případně mu sdělí další informace týkající se dodávky.

Veškerá komunikace mezi odběratelem a dodavatelem probíhá do uzavření výběrového řízení elektronicky prostřednictvím zpráv e-tržistiště. Provozovatel e-tržistiště je oprávněn požadovat od vítězné firmy provizi z každého uzavřeného obchodu, a to až do výše 3 % ceny zakázky. Výše provize je sjednána ve zprostředkovatelské smlouvě při jejím uzavírání.

Závěr

e-Government v ČR je teprve ve svých počátcích ačkoli transformace vlády na elektronickou začala již v roce 1999. Je to způsobeno nedostatečnou právní úpravou dané problematiky, která je šita horkou jehlou a doladěována za pochodu novelami odpovídajících legislativních norem. Také pomalé tempo zavádění ICT jak ve státní správě, tak i v soukromém sektoru a poměrně nízká odbornost odpovídajících pracovníků na straně státu i soukromého sektoru přispívá k pomalému rozvoji e-governmentu.

Na druhou stranu neexistence právních norem, které přikazují využívání služeb e-governmentu, umožňuje firmám využívat klasický papírový styk s úřady státní správy. Tuto situaci podporuje, dá se říci, až neochota firem využívat e-government i nízká úroveň elektronizace státní správy na úrovni vybavení ICT a vytvoření odpovídajících datových skladů.

Možným řešením této situace je přijetí takových legislativních norem, které jednoznačně upravují danou problematiku e-governmentu ať již na straně účetnictví, daní, obchodního práva, správního práva nebo na straně formální, kdy je jednoznačně dáno, jakým způsobem a za jakých podmínek lze komunikovat se státní správou, aby nedocházelo k různým výkladům odpovídajících zákonů.

Toto řešení je však velmi náročné na časové, finanční a lidské zdroje. Lze tedy předpokládat, že tento „bojový“ stav potrvá ještě několik let. Současnou nabídku služeb e-governmentu lze však považovat za dobrý počáteční krok, jak lze tyto služby provozovat a do budoucna zlepšovat a rozšiřovat.

Použité zdroje

- [1] Byznys rychlostí myšlenky - Bill Gates - Management Press, Ringier ČR a.s. ISBN 80-85943-97-2.
- [2] Digitální ekonomika - Don Tapscott - Computer Press – ISBN 80-7226-176-2.
- [3] Implementing and Managing eGovernment- Richard Heeks – Paperback ISBN 0761967923.
- [4] Nařízení vlády č. 304/2001 Sb. ze dne 25. 7. 2001
- [5] Sbírka zákonů - Ministerstvo vnitra ČR - ISSN 1211-1244
Zákon o elektronickém podpisu č. 227//2000 Sb. ze dne 29. 6. 2000
- [6] Vyhláška Úřadu pro ochranu osobních údajů č. 366/2001 Sb. ze dne 3. 10. 2001
- [7] Zákon č. 226/2002 ze dne 9. 5. 2002
- [8] Zákon č. 517/2002 ze dne 14. 11. 2002
- [9] Zákon č. 440/2004 ze dne 24. 6. 2004

Elektronické zdroje:

- [10] http://www.ica.cz/home_cs/
- [11] <https://www.eidentity.cz/Home.html>
- [12] <http://qca.postsignum.cz/uvod.php>
- [13] <http://www.micr.cz/>
- [14] Státní informační a komunikační politika e-Česko 2006 [online].[citace z 30. 11. 2006]. Dostupné z <<http://www.micr.cz/scripts/detail.php?id=275>>
- [15] http://portal.gov.cz/wps/portal/_s.155/6966/place
- [16] Portál veřejné správy České republiky - Provozní řád. [online] [cit. 8. 12. 2006]. Dostupné z:
<http://portal.gov.cz/wps/portal/_s.155/696/_s.155/7238?docid=102250>
- [17] https://bezpecne.podani.gov.cz/asp/registration_standard.asp
- [18] http://portal.gov.cz/wps/portal/_s.155/6966/_s.155/710/place